The Dynamic Analysis of WannaCry Ransomware

Da-Yu Kao*, Shou-Ching Hsiao**

**Department of Information Management, Central Police University, Taoyuan City 333, Taiwan*

***Haishan Precinct, New Taipei City Police Department, New Taipei City 220, Taiwan*

camel@mail.cpu.edu.tw, oliver84312@gmail.com

***Abstract*—The global ransomware cyberattacks cripples the national hospital system across the United Kingdom, and causes waves of appointments and operations to be cancelled. Similar attacking methods have come to sweep over the world. Such trend of high-profile cyberattack sheds the lights on rapid defence through the malware information sharing platform. A complete malware analysis process is quite a time-consuming campaign. The dynamic analysis of WannaCry ransomware explores behavioural indicators and extracts important IOCs (Indicators of Compromise). Utilizing Yara tool to create customized patterns is useful for malware information sharing mechanism. Also, such mechanism help reduce time and human resource spent on detecting or finding similar malware families. We aim to generate effective cyber threat intelligence by formulating collected IOCs into structured formations. The positive effects show on immediate defensive response to security breaches, and meanwhile the integrated information security protection is consolidated.**

***Keyword*—Cyber Threat Intelligence, Ransomware, Dynamic Analysis, Indicators of Compromise, Malware Information Sharing Platform**

Da-Yu Kao is an Associate Professor at Department of Information Management, Central Police University, Taiwan. With a Master degree in Information Management and a PhD degree in Crime Prevention and Correction, he had led several investigations in cooperation with police agencies from other countries for the past 20 years. He can be reached at camel@mail.cpu.edu.tw.

Shou-Ching Hsiao is an information lieutenant at Haishan Precinct, New Taipei City Police Department, Taiwan. She is responsible for information system management, information security, and real-time video for security control. She can be reached at oliver84312@gmail.com.